UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/743,756	12/24/2003	Steven N. Simon	P3136-938	8932

62665 7590 02/04/2011

BUCHANAN INGERSOLL & ROONEY, PC
1737 King Street, Suite 500
ALEXANDRIA, VA 22314

EXAMINER	
LI, GUANG W	

ART UNIT	PAPER NUMBER
2478	

NOTIFICATION DATE	DELIVERY MODE
02/04/2011	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

ADIPFDD@bipc.com
offserv@bipc.com

Office Action Summary	Application No.	Applicant(s)	
	10/743,756	SIMON ET AL.	
	Examiner	Art Unit	
	GUANG LI	2478	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *14 December 2010*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1,12,14,16,17,27,28,39,41,43,44,47,48,51-57 and 65* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1,12,14,16,17,27,28,39,41,43,44,47,48,51-57 and 65* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *24 December 2003* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. It is hereby acknowledged that the following papers have been received and placed of record in the file: Amendment date 12/14/2010

2. Claims 1, 12, 14, 16, 17, 27-28, 39, 41, 43-44, 47-48, 51-57 and 65 are presented for examination.

Response to Arguments

3. Applicant's arguments with respect to claims 1, 12, 14, 16, 17, 27-28, 39, 41, 43-44, 47-48, 51-57 and 65 have been considered but are moot in view of the new ground(s) of rejection.

Claim Rejections - 35 USC § 112

4. The following is a quotation of the first paragraph of 35 U.S.C. 112:

> The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

5. Claim 65 is rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the written description requirement. The claim(s) contains subject matter which was not described in the specification in such a way as to reasonably convey to one skilled in the relevant art that the inventor(s), at the time the application was filed, had possession of the claimed invention.

6. Claim 65 "the public key is shared by a plurality of server computers each respectively having different network addresses from each other" was not described in the specification. In the specification ¶[0020], applicant discloses "each replicated password server 14 has the same public key such that it can be used to identify all of the replicated password servers 14". At the

most, Applicant discloses each password server has the same public key, which lack of description of the public key is shared with a plurality of server computers.

Claim Rejections - 35 USC § 103

7. The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior Office action.

8. Claims 1, 12, 14, 16, 17, 27-28, 39, 41, 43-44, 47-48, 51-54 and 65 are rejected under 35 U.S.C. 103(a) as being unpatentable over Kumar et al. (US 6,795,434) in view of Robertson et al. (US 2003/0196107 A1).

9. Regarding claim 1, Kumar teaches a method for a client computer to find a network address of a password server computer having a public key, the method comprising:

searching for a network address (Best replicated server see Kumar: col.2 line 23) of the server computer using a backup search procedure if the address of the server computer cannot be identified using a primary search procedure (Searching the server's addresses using the initiate DNS lookup when the URL not found in the memory cache "The process proceeds to block 402 to examine whether the requested URL host name is in the local cache memory" see Kumar: col.5 lines 26-45; Fig. 4 steps 402-408); and

establishing a connection with the server computer using the network address found (Once detect the most preferred server address and establish to the server "The address listed on the top of the sorted preferred list is the most preferred server address, which points to the most preferred server or the optimal site is addressed by the most preferred server address" see Kumar: col.7 lines 48-56; Fig.4 Step 410),

wherein:

the backup search procedure searches for the server computer using the public key to identify the server computer (DNS lookup as backup search procedure "If the requested URL host name is not in the cache, the process proceeds from block 402 to block 404, where the process initiates a DNS lookup for the requested URL host name" see Kumar: col.5 lines 34-37).

Kumar does not explicitly to disclose the public key is an identifier of the server computer and the public key identifies a plurality of server computers having different network addresses.

However Robertson teaches the public key is an identifier of the server computer and the public key identifies a plurality of server computers having different network addresses (unique identifier name for the each IPSAP base server and server return IP addresses of the destination IPSAP based server and public "Each IPSAP base server is given a unique identifier name (net-id) and Pretty Good Privacy (PGP) public/private keys technology (IETF RFC 1991 PGP Message Exchange Formats) to identify … and then returning the IP addresses of the destination IPSAP based server the PGP public key for the requested IPSAP base server" see Robertson: ¶[0005]) in order to provide a workable system for allowing a user to authenticated across multiple IP networks and road at will (see Robertson: ¶[0004]).

It would have been obvious to one of ordinary skill in the art at the time of invention to create the invention of Kumar to include (or to use, etc.) the public key is an identifier of the server computer and the public key identifies a plurality of server computers having different network address as taught by Robertson in order to provide a workable system for allowing a user to authenticated across multiple IP networks and road at will (see Robertson: ¶[0004]).

10. Regarding claim 12, the modified Kumar taught the method of claim 1 as described hereinabove. Robertson further comprising authenticating the server computer after the connection has been established (remote authentication the IPSAP base server when allowing building trust relationship between server and client "Remote Authentication Dial In User Service (RADIUS) authentication (IETF RFC 2138) is used to interface the IPSAP base server with the existing authentication program" see Robertson: ¶[0005]).

11. Regarding claim 14, the modified Kumar taught the method of claim 1 as described hereinabove. Kumar further comprising the step of populating a local storage of the client computer with a list of network addresses for server computers after the connection has been established (update the list of the server network address "At block 854, the process sorts the addresses into a preferred list of site addresses according to the responses and data types" see Kumar: col.9 lines 14-21).

12. Regarding claim 16, the modified Kumar taught the method of claim 1 as described hereinabove. Kumar further teaches wherein the primary and backup search procedures are performed in parallel (either can based on hit and miss ratio or DNS lookup "the comparing unit 506 issues a message of cache-miss to indicate that IP server addresses are not in the cache 522. Both the message of cache-miss and the message of cache-hit, which could be configured to one message, are sent to the selecting unit 510 and DNS lookup unit 508" see Kumar: col.6 lines 44-47).

13. Regarding claim 17, claim 17 is rejected for the same reason as claim 1 as set forth hereinabove.

14. Regarding claim 27, claim 27 is rejected for the same reason as claim 16 as set forth hereinabove.

15. Regarding claim 28, claim 28 is rejected for the same reason as claim 1 as set forth hereinabove.

16. Regarding claim 39, claim 39 is rejected for the same reason as claim 12 as set forth hereinabove.

17. Regarding claim 41, claim 41 is rejected for the same reason as claim 14 as set forth hereinabove.

18. Regarding claim 43, claim 43 is rejected for the same reason as claim 16 as set forth hereinabove.

19. Regarding claim 44, Kumar teaches a method for a client computer to locate a network address of a server computer on a computer network, said server computer having a public key that is an identifier of the server computer, the method comprising:

searching for the address of the server computer in a local system storage of the client computer (Searching the URL in the memory cache "The process proceeds to block 402 to examine whether the requested URL host name is in the local cache memory" see Kumar: col.5 lines 27-28); and

performing a backup search procedure if the address is not found in the local system storage (DNS lookup as backup search procedure "If the requested URL host name is not in the cache, the process proceeds from block 402 to block 404, where the process initiates a DNS lookup for the requested URL host name" see Kumar: col.5 lines 34-37),

the backup search procedure being selected from a group of search procedures including the following:

broadcasting a message over the network to identify the address of the server computer,

searching an authentication record for the address of the server computer (DNS lookup in the server computer for relating to the requested URL is selected when URL not found in the local memory "Upon initiating a DNS lookup, DNS searches and collects addresses relating to the requested URL host name" see col.5 lines 38-40),

using a loop back address,

using a inter process communication to determine whether the server computer is running on a same CPU as the client computer in order to determine the network address, and

searching a configuration record of the client computer for the address of the server computer; and

establishing a connection with the server computer using the network address found (Once detect the most preferred server address and establish to the server "The address listed on the top of the sorted preferred list is the most preferred server address, which points to the most preferred server or the optimal site is addressed by the most preferred server address" see Kumar: col.7 lines 48-56; Fig.4 Step 410).

Kumar does not explicitly to disclose the one or more of said search procedures searches for the server computer using the public key to identify the server computer, and the public key identifies a plurality of server computers having different network addresses.

However Robertson teaches the one or more of said search procedures searches for the server computer using the public key to identify the server computer, and the public key

identifies a plurality of server computers having different network addresses (unique identifier name for the each IPSAP base server and server return IP addresses of the destination IPSAP based server and public key "Each IPSAP base server is given a unique identifier name (net-id) and Pretty Good Privacy (PGP) public/private keys technology (IETF RFC 1991 PGP Message Exchange Formats) to identify … and then returning the IP addresses of the destination IPSAP based server the PGP public key for the requested IPSAP base server" see Robertson: ¶[0005]) in order to provide a workable system for allowing a user to authenticated across multiple IP networks and road at will (see Robertson: ¶[0004]).

It would have been obvious to one of ordinary skill in the art at the time of invention to create the invention of Kumar to include (or to use, etc.) the one or more of said search procedures searches for the server computer using the public key to identify the server computer, and the public key identifies a plurality of server computers having different network addresses as taught by Robertson in order to provide a workable system for allowing a user to authenticated across multiple IP networks and road at will (see Robertson: ¶[0004]).

20. Regarding claim 47, claim 47 is rejected for the same reason as claim 16 as set forth hereinabove.

21. Regarding claim 48, Kumar teaches a system for finding a network address, the system comprising:

client means for:

searching for the network address (Best replicated server see Kumar: col.2 line 23) of the server means by searching for the address of the server means in a local system storage of the client means (Searching the server's addresses using the initiate DNS lookup when the URL not

found in the memory cache "The process proceeds to block 402 to examine whether the requested URL host name is in the local cache memory" see Kumar: col.5 lines 26-45; Fig. 4 steps 402-408),

using a backup search procedure to identify the address of the server means if the address is not found in the local system storage (DNS lookup as backup search procedure "If the requested URL host name is not in the cache, the process proceeds from block 402 to block 404, where the process initiates a DNS lookup for the requested URL host name" see Kumar: col.5 lines 34-37), and

establishing a connection with the server means using the network address found (Once detect the most preferred server address and establish to the server "The address listed on the top of the sorted preferred list is the most preferred server address, which points to the most preferred server or the optimal site is addressed by the most preferred server address" see Kumar: col.7 lines 48-56; Fig.4 Step 410),

wherein the client means is configured to search for the network address as the backup search, the backup procedure being selected from a group of search procedures including the following:

broadcast a message over the network to find the address of the server means,

search an authentication record for the address of the server means (DNS lookup in the server computer for relating to the requested URL is selected when URL not found in the local memory "Upon initiating a DNS lookup, DNS searches and collects addresses relating to the requested URL host name" see col.5 lines 38-40),

use a loop back address,

use a inter process communication to determine whether the server means is running on a CPU that is the same CPU on which the client is running means in order to determine the network address, and

search a configuration record of the client means for the address of the server means.

Kumar does not explicitly to disclose the server means having a network address and a public key, the public key being an identifier of the server means; one or more of said search procedures searches for the server means using the public key to identify the server means, and the public key identifies a plurality of server computers having different network addresses.

However Robertson teaches the server means having a network address and a public key, the public key being an identifier of the server means; one or more of said search procedures searches for the server means using the public key to identify the server means, and the public key identifies a plurality of server computers having different network addresses (unique identifier name for the each IPSAP base server and server return IP addresses of the destination IPSAP based server and public key "Each IPSAP base server is given a unique identifier name (net-id) and Pretty Good Privacy (PGP) public/private keys technology (IETF RFC 1991 PGP Message Exchange Formats) to identify ... and then returning the IP addresses of the destination IPSAP based server the PGP public key for the requested IPSAP base server" see Robertson: ¶[0005]) in order to provide a workable system for allowing a user to authenticated across multiple IP networks and road at will (see Robertson: ¶[0004]).

It would have been obvious to one of ordinary skill in the art at the time of invention to create the invention of Kumar to include (or to use, etc.) server means having a network address and a public key, the public key being an identifier of the server means; one or more of said

search procedures searches for the server means using the public key to identify the server means, and the public key identifies a plurality of server computers having different network addresses as taught by Robertson in order to provide a workable system for allowing a user to authenticated across multiple IP networks and road at will (see Robertson: ¶[0004]).

22. Regarding claim 51, claim 51 is rejected for the same reason as claim 16 as set forth hereinabove.

23. Regarding claim 52, Kumar teaches a method for a client computer to find a network address of a server computer, the method comprising:

performing a primary search procedure, the primary search procedure including searching a local storage of the client computer system for the network address of the server computer (Searching the URL in the memory cache "The process proceeds to block 402 to examine whether the requested URL host name is in the local cache memory" see Kumar: col.5 lines 27-28);

performing a backup search procedure if the network address of the server computer is not found using the primary search procedure DNS lookup as backup search procedure "If the requested URL host name is not in the cache, the process proceeds from block 402 to block 404, where the process initiates a DNS lookup for the requested URL host name" see Kumar: col.5 lines 34-37) and

establishing a connection with the server computer using the network address found (Once detect the most preferred server address and establish to the server "The address listed on the top of the sorted preferred list is the most preferred server address, which points to the most

preferred server or the optimal site is addressed by the most preferred server address" see Kumar: col.7 lines 48-56; Fig.4 Step 410).

Kumar does not explicitly disclose the backup search procedure including searching a configuration record of the client computer system for the network address of the server computer.

However Robertson teaches the he backup search procedure including searching a configuration record of the client computer system for the network address of the server computer (Software on the user's computer also determines additional public information about the IP network and then acquires configuration information from the IPSAP central server and the local IPSAP base server" see Kumar: ¶[0007]) in order to provide a workable system for allowing a user to authenticated across multiple IP networks and road at will (see Robertson: ¶[0004]).

It would have been obvious to one of ordinary skill in the art at the time of invention to create the invention of Kumar to include (or to use, etc.) the backup search procedure including searching a configuration record of the client computer system for the network address of the server computer as taught by Robertson in order to provide a workable system for allowing a user to authenticated across multiple IP networks and road at will (see Robertson: ¶[0004]).

24. Regarding claim 53, Kumar teaches the method of claim 52 as described hereinabove. Robertson further teaches the server computer is a password server computer having a public key that is an identifier of the server computer and the primary search procedure or the backup search procedure searches for the server computer using the public key to identify the server computer, said public key identifying a plurality of server computers having different network addresses.

(unique identifier name for the each IPSAP base server "Each IPSAP base server is given a unique identifier name (net-id) and Pretty Good Privacy (PGP) public/private keys technology (IETF RFC 1991 PGP Message Exchange Formats) to identify … and then returning the IP addresses of the destination IPSAP based server the PGP public key for the requested IPSAP base server" see Robertson: ¶[0005]).

25. Regarding claim 54, Kumar teaches a method for a client computer to find a network address of a server computer, the method comprising:

performing a primary search procedure Searching the URL in the memory cache "The process proceeds to block 402 to examine whether the requested URL host name is in the local cache memory" see col.5 lines 27-28);

performing a backup search procedure if the network address of the server computer is not found using the primary search procedure (DNS lookup as backup search procedure "If the requested URL host name is not in the cache, the process proceeds from block 402 to block 404, where the process initiates a DNS lookup for the requested URL host name see col.5 lines 34-37"), and

establishing a connection with the server computer using the network address found (Once detect the most preferred server address and establish to the server "The address listed on the top of the sorted preferred list is the most preferred server address, which points to the most preferred server or the optimal site is addressed by the most preferred server address" see Kumar: col.7 lines 48-56; Fig.4 Step 410).

Kumar does not explicitly disclose backup search procedure searching an authentication record for the network address of the server computer.

However Robertson teaches the backup search procedure searching an authentication record for the network address of the server computer (remote authentication the IPSAP base server when allowing building trust relationship between server and client "Remote Authentication Dial In User Service (RADIUS) authentication (IETF RFC 2138) is used to interface the IPSAP base server with the existing authentication program" see Robertson: ¶[0005]) in order to provide a workable system for allowing a user to authenticated across multiple IP networks and road at will (see Robertson: ¶[0004]).

It would have been obvious to one of ordinary skill in the art at the time of invention to create the invention of Kumar to include (or to use, etc.) the backup search procedure searching an authentication record for the network address of the server computer as taught by Robertson in order to provide a workable system for allowing a user to authenticated across multiple IP networks and road at will (see Robertson: ¶[0004]).

26. Regarding claim 65, Kumar teaches a method for a client computer to find a network address of a password server computer having a public key, the method comprising:

searching for a network address of the server computer using a backup search procedure if the address of the server computer cannot be identified using a primary search procedure (DNS lookup as backup search procedure "If the requested URL host name is not in the cache, the process proceeds from block 402 to block 404, where the process initiates a DNS lookup for the requested URL host name" see Kumar: col.5 lines 34-37); and

establishing a connection with the server computer using the network address found (Once detect the most preferred server address and establish to the server "The address listed on the top of the sorted preferred list is the most preferred server address, which points to the most

preferred server or the optimal site is addressed by the most preferred server address" see Kumar: col.7 lines 48-56; Fig.4 Step 410).

Kumar does not explicitly to disclose the public key to identify the server computer, and the public key is shared by a plurality of server computers each respectively having different network addresses from each other.

However Robertson teaches the public key to identify the server computer, and the public key is shared by a plurality of server computers each respectively having different network addresses from each other (unique identifier name for the each IPSAP base server and server return IP addresses of the destination IPSAP based server and public key and the PGP Public key for the requested IPSAP base server "Each IPSAP base server is given a unique identifier name (net-id) and Pretty Good Privacy (PGP) public/private keys technology (IETF RFC 1991 PGP Message Exchange Formats) to identify … and then returning the IP addresses of the destination IPSAP based server the PGP public key for the requested IPSAP base server" see Robertson: ¶[0005]) in order to provide a workable system for allowing a user to authenticated across multiple IP networks and road at will (see Robertson: ¶[0004]).

It would have been obvious to one of ordinary skill in the art at the time of invention to create the invention of Kumar to include (or to use, etc.) the one or more of said search procedures searches for the server computer using the public key to identify the server computer, and the public key identifies a plurality of server computers having different network addresses as taught by Robertson in order to provide a workable system for allowing a user to authenticated across multiple IP networks and road at will (see Robertson: ¶[0004]).

27. Claims 55 and 57 are rejected under 35 U.S.C. 103(a) as being unpatentable over Kumar et al. (US 6,795,434) in view of Gulko et al. (US 2003/0177240 A1).

28. Regarding claim 55, Kumar teaches a method for a client computer to find a network address of a server computer, the method comprising:

performing a primary search procedure (Searching the URL in the memory cache "The process proceeds to block 402 to examine whether the requested URL host name is in the local cache memory" see col.5 lines 27-28);

performing a backup search procedure if the network address of the server computer is not found using the primary search procedure (DNS lookup as backup search procedure "If the requested URL host name is not in the cache, the process proceeds from block 402 to block 404, where the process initiates a DNS lookup for the requested URL host name see col.5 lines 34-37"), and

establishing a connection with the server computer using the network address found (Once detect the most preferred server address and establish to the server "The address listed on the top of the sorted preferred list is the most preferred server address, which points to the most preferred server or the optimal site is addressed by the most preferred server address" see Kumar: col.7 lines 48-56; Fig.4 Step 410).

Kumar does not explicitly to disclose the backup search procedure determining whether the server computer is running on a CPU that is the same CPU on which the client computer is running in order to determine the network address of the server computer.

However Gulko teaches t backup search procedure determining whether the server computer is running on a CPU that is the same CPU on which the client computer is running in

order to determine the network address of the server computer (whether the resource on the same processor by using inter process communication (IPC) "That resource can be the same or another processor resident on the machine that is executing application 60, or can be another machine connected via a network 4" see Gulko: ¶[0137]; ¶[0151]) in order to reduction computation time and increase in result accuracy (see Gulko: ¶[0012]).

It would have been obvious to one of ordinary skill in the art at the time of invention to create the invention of Kumar to include (or to use, etc.) the public key is an identifier of the server computer and the public key identifies a plurality of server computers having different network address as taught by Gulko in order to reduction computation time and increase in result accuracy (see Gulko: ¶[0012]).

29. Regarding claim 57, the modified Kumar taught the method of claim 55 as described hereinabove. Gulko further teaches the step of determining whether the server computer is running on the same CPU of the client computer comprises sending out an inter process communication to the CPU (whether the resource on the same processor by using inter process communication (IPC) "That resource can be the same or another processor resident on the machine that is executing application 60, or can be another machine connected via a network 4" see Gulko: ¶[0137]; ¶[0151]).

30. Claims 56 is rejected under 35 U.S.C. 103(a) as being unpatentable over Kumar et al. (US 6,795,434) in view of Gulko et al. (US 2003/0177240 A1) and further in view of Lavian (US 7, 039,724)

31. Regarding claim 56, the modified Kumar taught the method of claim 55 as described hereinabove. The modified Kumar does not teaches the step of determining whether the server computer is running on the same CPU as the client computer comprises using a loop back address of the server computer.

However Lavian further teaches wherein determining whether the server computer is running on the same CPU as the client computer comprises: using a loop back address of the server computer (using the loopback address to test whether the device is local node or not "This loopback address is a self-referential address which identifies the local network device on the network without sending packets of information over the actual network" see Lavian: col. 10 lines 44-50) in order to provide alternate way to finding network address for fault tolerant purpose of Lavian.

It would have been obvious to one of ordinary skill in the art at the time of invention to create the invention of the modified Kumar to include (or to use, etc.) the public key is an identifier of the server computer and the public key identifies a plurality of server computers having different network address as taught by Lavian in order to provide alternate way to finding network address for fault tolerant purpose of Lavian.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Guang Li whose telephone number is (571) 270-1897. The examiner can normally be reached on Monday-Friday 8:30AM-5:00PM(EST).

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Jeff Pwu can be reached on (571) 272-6798. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

GL
Patent Examiner

January 31, 2011

/Jeffrey Pwu/

Supervisory Patent Examiner, Art Unit

2478